Docket No.: SON-2934
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Takeshi Kokubo

Art Unit: N/A

Application No.: Not Yet Assigned

Filed: March 3, 2004

For: MOBILE TERMINAL APPARATUS

CLAIM FOR PRIORITY AND SUBMISSION OF DOCUMENTS

MS Patent Application
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicant hereby claims priority under 35 U.S.C. 119 based on the following prior foreign application filed in the following foreign country on the date indicated:

Country	Application No.	Date
Japan	P2003-061233	March 7, 2003

In support of this claim, a certified copy of the said original foreign application is filed herewith.

Dated: March 3, 2004

Respectfully submitted,

By Robert S. Green Reg No. 41,800
Ronald P. Kananen
Registration No.: 24,104
(202) 955-3750
Attorneys for Applicant

SOFP0310KK00

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application:	２００３年　３月　７日
出願番号 Application Number:	特願２００３－０６１２３３
[ST. 10/C]:	[ＪＰ２００３－０６１２３３]
出願人 Applicant(s):	ソニー・エリクソン・モバイルコミュニケーションズ株式会社

２００３年１２月１９日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００３－３１０５４７５

【書類名】　特許願
【整理番号】　0200097806
【あて先】　特許庁長官　殿
【国際特許分類】　H04M　1/66
【発明者】
　【住所又は居所】　東京都港区港南１丁目８番１５号　ソニー・エリクソン・モバイルコミュニケーションズ株式会社内
　【氏名】　小久保　武
【特許出願人】
　【識別番号】　501431073
　【氏名又は名称】　ソニー・エリクソン・モバイルコミュニケーションズ株式会社
【代理人】
　【識別番号】　100098350
　【弁理士】
　【氏名又は名称】　山野　睦彦
　【電話番号】　0466-28-6817
【手数料の表示】
　【予納台帳番号】　054254
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　0202008
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　移動端末装置

【特許請求の範囲】

【請求項１】

データを記憶する記憶手段と、

通信ネットワークを介してデータの通信を行う通信手段と、

ユーザの操作に基づいてそのユーザが正当なユーザであるか否かをチェックする認証手段と、

この認証手段による認証の結果が否定的であるとき、前記通信手段により、前記記憶手段に記憶されたデータのうち、予め定められたデータを、予め定められたサーバに対して送信し、この送信完了後に前記予め定められたデータを前記記憶手段から消去する制御手段と、

を備えたことを特徴とする移動端末装置。

【請求項２】

前記予め定められたデータとして、ユーザが所望のデータを指定する手段を備えたことを特徴とする請求項１記載の移動端末装置。

【請求項３】

前記認証手段による認証処理は前記予め定められたデータにユーザがアクセスしようとしたとき行われることを特徴とする請求項１または２記載の移動端末装置。

【請求項４】

データの種類に応じて前記サーバへの送信後のデータの消去処理を省略することを特徴とする請求項１記載の移動端末装置。

【請求項５】

データを記憶する記憶手段と、

通信ネットワークを介して電子メールの通信を行う通信手段と、

受信した電子メールにより予め定められた指示を受信したとき、前記予め定められたデータを予め定められたサーバに対して送信し、この送信完了後に前記予め定められたデータを前記記憶手段から消去する制御手段と、

を備えたことを特徴とする移動端末装置。

【請求項６】

前記制御手段は、前記サーバへのデータの送信の前提として、前記電子メールの発信者情報が予め登録されている発信者情報と一致すること、前記電子メールが所定時間内に所定回数受信されること、の少なくとも一つの条件を課すことを特徴とする請求項５記載の移動端末装置。

【請求項７】

データの種類に応じて前記サーバへの送信後のデータの消去処理を省略することを特徴とする請求項５記載の移動端末装置。

【請求項８】

データを記憶する記憶手段と、

電話の自動着信を行う手段と、

自動着信時にトーン信号入力を受け付ける手段と、

予め定められたトーン信号列を受信したとき前記予め定められたデータを予め定められたサーバに対して送信し、この送信完了後に前記予め定められたデータを前記記憶手段から消去する制御手段と、

を備えたことを特徴とする移動端末装置。

【請求項９】

データの種類に応じて前記サーバへの送信後のデータの消去処理を省略することを特徴とする請求項８記載の移動端末装置。

【請求項１０】

データを記憶する記憶手段と、

通信ネットワークを介してデータの通信を行う通信手段と、

ユーザの操作に基づいてそのユーザが正当なユーザであるか否かをチェックする認証手段と、

この認証手段による認証の結果が否定的であるとき、前記通信手段により、前記記憶手段に記憶されたデータのうち、予め定められたデータを、予め定められたサーバに対して送信する制御手段と、

を備えたことを特徴とする移動端末装置。

【請求項１１】

前記制御手段は認証の結果が否定的であるとき、少なくとも一定時間、当該データのアクセスのための認証処理自体の実行を抑止することを特徴とする請求項１０記載の移動端末装置。

【請求項１２】

認証手段を複数有し、

前記制御手段は認証の結果が否定的であるとき、より高度な認証手段の利用に切り替えることを特徴とする請求項１０記載の移動端末装置。

【請求項１３】

データを記憶する記憶手段と、

前記記憶手段に記憶されたデータのうち、予め定められたまたは予め指定されたデータにユーザがアクセスしようとしたとき、予め定められたユーザの操作に基づいてそのユーザが正当なユーザであるか否かをチェックする認証手段と、

この認証の結果が否定的であるとき、少なくとも一定時間、当該データのアクセスのための認証処理自体の実行を抑止する制御手段と、

を備えたことを特徴とする移動端末装置。

【請求項１４】

データを記憶する記憶手段と、

前記記憶手段に記憶されたデータのうち、予め定められたまたは予め指定されたデータにユーザがアクセスしようとしたとき、予め定められたユーザの操作に基づいてそのユーザが正当なユーザであるか否かをチェックするための複数の認証手段と、

認証の結果が否定的であるとき、より高度な認証手段の利用に切り替える制御手段と、

を備えたことを特徴とする移動端末装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、携帯電話機や携帯情報端末（ＰＤＡ）等の移動端末装置（本明細書

では、端末装置を単に端末ともいう）に関する。

【０００２】

【従来の技術】

携帯電話機や携帯情報端末（ＰＤＡ）等の移動端末は、携帯されるが故に、紛失、盗難等の事態が不可避的に発生する。また、移動端末は通常個人で利用されるものであり、電話帳データ、メモデータ、電子メールデータ等の個人情報が保存されているため、端末の盗難、紛失等があった場合には、そのような個人情報等のデータの不正閲覧、改竄等のおそれが生じる。

【０００３】

従来、必要な場合、各種認証の導入により端末内データへの不正アクセスに関するセキュリティーの確保が図られているが、個人情報等の重要性を考えると、従来の認証方法だけでは必ずしも十分ではない。

【０００４】

特許文献１には、移動端末機のような移動端末が紛失したことの届け出が移動端末の位置登録局にあった場合、位置登録局はその移動端末が基地局と交信したときに、基地局からの制御信号によりその移動端末のキー操作を無効にするとともに、内部のデータを位置登録局のデータベースに転送させた後、移動端末内でそのデータを消去させる技術を開示している。

【０００５】

【特許文献１】

特開２００１－３０９４３１号公報

【０００６】

【発明が解決しようとする課題】

特許文献１の技術では、位置登録局および基地局が特別な処理を行わなければならない。すなわち、位置登録局において紛失等の届け出のあった移動端末の管理およびチェックを行い、紛失等の届け出のあった移動端末が基地局と交信した際には移動端末の操作を無効にしたり、データを転送させるための信号の生成および制御という特別な処理を行わなければならない。また、ユーザが届け出を行う必要があり、届け出事項が位置登録局および基地局の処理に反映されるまでに

遅延が生じるという問題もある。

【０００７】

本発明はこのような背景においてなされたものであり、その目的は、位置登録局や基地局による特別な処理を必要とすることなく、内部のデータを不正に閲覧しようとする者からデータを保護することができる移動端末装置を提供することにある。

【０００８】

本発明による他の目的は、データを保護すべき事態が生じたとき、または、その自体に気づいたとき、即座にデータの保護を行うことができる移動端末装置を提供することにある。

【０００９】

本発明によるさらに他の目的は、端末紛失等の場合も端末内のデータの利用を確保することができる移動端末装置を提供することにある。

【００１０】

【課題を解決するための手段】

本発明による移動端末装置は、データを記憶する記憶手段と、通信ネットワークを介してデータの通信を行う通信手段と、ユーザの操作に基づいてそのユーザが正当なユーザであるか否かをチェックする認証手段と、この認証手段による認証の結果が否定的であるとき、前記通信手段により、前記記憶手段に記憶されたデータのうち、予め定められたデータを、予め定められたサーバに対して送信し、この送信完了後に前記予め定められたデータを前記記憶手段から消去する制御手段とを備えたことを特徴とする。

【００１１】

ユーザの操作により認証手段により認証処理が行われ、その結果が否定的であったとき、制御手段は、記憶手段内の予め定められたデータをサーバに対して送信することにより、当該データを待避し、その後、当該データを消去する。これにより、当該データは不正な閲覧・使用等から有効に保護される。

【００１２】

前記予め定められたデータは、デフォルトで定まっていてもよいが、ユーザが

所望のデータを指定する手段を備えることが好ましい。これにより、デフォルトで定めっていないデータも保護の対象とすることができる。

【００１３】

前記認証手段による認証処理は、例えば、前記予め定められたデータにユーザがアクセスしようとしたとき行われる。

【００１４】

データの種類に応じては、前記サーバへの送信後のデータの消去処理を省略することも可能である。データの消去を行うと、後にデータの復帰処理が必要となる。データの重要性等に応じて、データの待避は行っても消去を行うほどではないというデータについては、消去を省略すれば、復帰処理が不要となる。

【００１５】

本発明による他の移動端末装置は、データを記憶する記憶手段と、通信ネットワークを介して電子メールの通信を行う通信手段と、受信した電子メールにより予め定められた指示を受信したとき、前記予め定められたデータを予め定められたサーバに対して送信し、この送信完了後に前記予め定められたデータを前記記憶手段から消去する制御手段とを備えたことを特徴とする。

【００１６】

この発明は、移動端末装置の紛失等に、正当ユーザが気づいたときに、当該正当ユーザが遠隔的に端末装置内のデータの待避および消去を指示するものである。その一つの方法が電子メールを用いるものである。この場合、前記制御手段は、前記サーバへのデータの送信の前提として、前記電子メールの発信者情報が予め登録されている発信者情報と一致すること、前記電子メールが所定時間内に所定回数受信されること、の少なくとも一つの条件を課すようにしてもよい。これにより、外部からの不正な指示を排除する。

【００１７】

当該正当ユーザが遠隔的に端末装置内のデータの待避および消去を指示する他の方法は電話によるトーン信号列を用いるものである。すなわち、この移動端末装置は、データを記憶する記憶手段と、電話の自動着信を行う手段と、自動着信時にトーン信号入力を受け付ける手段と、予め定められたトーン信号列を受信し

たとき前記予め定められたデータを予め定められたサーバに対して送信し、この送信完了後に前記予め定められたデータを前記記憶手段から消去する制御手段とを備えたことを特徴とする。

【００１８】

上記移動端末装置において、データの消去は必須ではなく、認証手段による認証の結果が否定的であるとき、前記通信手段により、前記記憶手段に記憶されたデータのうち、予め定められたデータを、予め定められたサーバに対して送信するのみでもよい。これにより、サーバに一旦データが待避されることになるので、当該データの利用が確保される。

【００１９】

前記制御手段は認証の結果が否定的であるとき、少なくとも一定時間、当該データのアクセスのための認証処理自体の実行を抑止するようにしてもよい。この発明では、データの待避および消去は行わず、認証処理自体の実行を抑止することにより、認証のリトライの機会を低減させるものである。認証手段を複数有する場合には、前記制御手段は認証の結果が否定的であるとき、より高度な認証手段の利用に切り替えるようにしてもよい。これにより、認証のリトライの成功率が低下する。

【００２０】

このような認証処理自体の抑止や認証手段の切替は、サーバへのデータの送信（アップロード）やデータの消去を行わない場合にも有効である。

【００２１】

【発明の実施の形態】

以下、本発明の実施の形態について、図面を参照して詳細に説明する。

【００２２】

図１に、本発明が適用されるシステムのモデル例を示す。本実施の形態では携帯電話機である移動端末１００と、基地局／制御局２００とサーバ３００とからなる。本実施の形態では、基地局と制御局は、便宜上一つのものとして、両者の機能を併せ持つものとして示している。サーバ３００は、基地局／制御局２００と、直接接続して示してあるが、ゲートウェイおよび公衆回線網等の通信ネット

ワークを介して接続されてもよい。

【００２３】

図２に、移動端末１００の構成例を示す。制御部１２０は、制御ライン１５０およびデータライン１６０を介して、移動端末１００の各部の制御を行う。通信回路１０２は、制御ライン１５０に接続され、アンテナ１０１を介して基地局／制御局２００との間で音声およびデータの通信を行う。表示部１０７は、例えば液晶ディスプレイのような表示デバイスを有し、制御ライン１５０およびデータライン１６０に接続され、各種の情報を表示する。操作部１０６は、各種操作キーやジョグダイヤル等を有し、制御ライン１５０に接続され、ユーザからの入力操作を受け付ける。メモリ１０５は、ＲＯＭ，ＲＡＭ，フラッシュメモリ等の記憶装置を有し、制御ライン１５０およびデータライン１６０に接続され、各種プログラムやデータを記憶する。メモリ１０５は後述するデータ保持部を構成している。報知部１０８は、バイブレータ、ＬＥＤ等からなり、制御ライン１５０に接続されて、選択的な着信通知等のためにユーザへの報知を行う。マイク１０３およびスピーカ１０４はデータライン１６０に接続され、音声の入出力を行う。

【００２４】

図３に基地局／制御局２００の構成例を示す。制御部２０３は、制御ライン２５０およびデータライン２６０を介して、基地局／制御局２００の各部の制御を行う。通信回路２０２は、制御ライン２５０に接続され、アンテナ２０１を介して移動端末１００との間で音声およびデータの通信を行う。メモリ２０４は、ＲＯＭ，ＲＡＭ，フラッシュメモリ等の記憶装置を有し、制御ライン２５０およびデータライン２６０に接続され、各種プログラムやデータを格納する。有線伝送路インタフェース（Ｉ／Ｆ）２０５は、制御ライン２５０およびデータライン２６０に接続され、有線伝送路２０６を介して外部装置と接続される。

【００２５】

図４は、サーバ３００の構成例を示す。制御部３０３は、制御ライン３５０およびデータライン３６０を介して、サーバ３００の各部の制御を行う。有線伝送路インタフェース（Ｉ／Ｆ）３０１は、制御ライン３５０およびデータライン３６０に接続され、有線伝送路３０６を介して外部装置と接続される。メモリ３０

４は、ＲＯＭ，ＲＡＭ，フラッシュメモリ等の記憶装置を有し、制御ライン３５０およびデータライン３６０に接続され、各種プログラムやデータを格納する。外部記憶装置３０２は、ハードディスク装置等の大容量記憶装置であり、制御ライン３５０およびデータライン３６０に接続されている。操作部３０５は、キーボード、ポインティングデバイス等の入力手段を有し、ユーザからの入力操作を受け付ける。図示しないが、サーバ３００は、さらに、表示デバイスを含む表示部を有してもよい。

【００２６】

以下、本実施の形態の動作を説明する。本実施の形態では、所定の条件に従って、原則的には、移動端末１００内のデータをサーバへ送信するアップロードを行い、その後、移動端末内の当該データを消去する。本実施の形態におけるアップロードはデータの待避の意味を有する。以下、アップロードの契機となる要因別に３つの例を説明する。

【００２７】

本実施の形態においてアップロードの対象となるデータは、データ保持部内の予め定められたデータまたはデータのフォルダ（メールボックス等を含む）であってもよいし、これに加えてまたはこれに代えて、ユーザが任意のデータやフォルダを指定できるようにしてもよい。これらのアップロードの対象となるデータを本明細書では「指定データ」という。

【００２８】

図５は、第１のアップロード処理の処理例を示している。

【００２９】

少なくとも第１のアップロード処理を採用する場合には、アップロードの対象となるデータへのアクセスに際して、認証が行われるものとする。すなわち、データの閲覧等のアクセスに対して、初期的に認証を必要としないデータであっても、アップロードの対象として指定されたデータについてはそのアクセスに対して認証を要求するよう、その指定に伴って自動的に設定されるものとする。認証はそのデータへアクセスすることに対する正当な権限を有することを確認するための処理であり、携帯端末では通常、パスワードの入力、照合によって行われる

。但し、認証の方法はパスワードに限るものではない。

【００３０】

図５において、ユーザにより、予め定められた指定データへのアクセスが行われようとしたとき（Ｓ５０１，Ｙｅｓ）、認証処理が起動される（Ｓ５０２）。例えば、ユーザに対してパスワードの入力が要求され、入力されたパスワードと登録されているパスワードとが照合される（Ｓ５０２）。両パスワードが一致したら、認証ＯＫと判断して（Ｓ５０３，Ｙｅｓ）、そのデータを表示し必要に応じてデータの追加、変更、削除等のユーザ操作を許容する（Ｓ５０９）。予め定められた回数のキーワード不一致が生じたら（Ｓ５０３，Ｎｏ）、認証誤りと判断し、キー操作を無効化する（Ｓ５０４）。これにより、一時的にユーザによるキー操作が受け付け不能となる。ネットワークへアクセスして当該指定データをサーバへ送信する（Ｓ５０５）。サーバのアクセス情報は予め移動端末内に保存されており、移動端末の正当なユーザは当該サーバにより提供されるサービスについてユーザ登録がなされているものとする。このデータの送信が終了したら（Ｓ５０６，Ｙｅｓ）、移動端末内の当該指定データを消去する（Ｓ５０７）。その後、キー操作無効化を解除して（Ｓ５０８）、本処理を終了する。

【００３１】

これによって、パスワードを知らない者が不当に前記指定データを閲覧等しようとしたときに、認証誤りを契機に、当該指定データがサーバにいわば「吸い上げ」られてしまうため、ユーザによる当該指定データに対する不当なアクセスが未然に防止されることになる。この吸い上げられたデータは、後述するように、その後、正当なユーザにより、その手元に戻った同移動端末または別の新たな端末にダウンロードすることができる。

【００３２】

図５に示した第１のアップロード処理は、移動端末に対する不正アクセスを契機として機能するものであったが、移動端末の正当なユーザが紛失等した当該移動端末を通信ネットワークを介して遠隔的に制御して、指定データのアップロードおよび消去を行わせることもできる。このような第２のアップロード処理を図６により説明する。

【００３３】

第２のアップロード処理は、データのアップロードを行うべき移動端末に対して、正当ユーザが所定の電子メール（本明細書では単にメールともいう）を発信することにより起動するものである。そのために、電子メールのヘッダ情報に所定のキーワードを含める。例えば、電子メールの「主題」の欄に「＊アップロード」のような文字列を含めて、当該移動端末のメールアドレス宛にメールを送信する。メールの「本文」欄は空欄であっても、あるいは定型文を予め埋め込んでおいてもよい。このようなメールは予め移動端末内に用意しておくことができる。キーワードは当該正当ユーザが移動端末内に予め設定しておくものとする。

【００３４】

図６において、移動端末は、メール着信を受けると（Ｓ６０１，Ｙｅｓ）、受信メールのヘッダ情報をチェックする（Ｓ６０２）。このチェックの結果、このメールがアップロード指示メールでなければ（Ｓ６０３，Ｎｏ）、通常のメール処理を行う（Ｓ６１１）。アップロード指示メールであれば（Ｓ６０３，Ｙｅｓ）、所定の条件が満足されたかをチェックする（Ｓ６０４）。この「所定の条件」の判断は、ヘッダ情報チェックに対してさらに別の認証機能を追加するものである。例えば、所定条件として、当該メールの発信者情報（発信者メールアドレス、発信者名等）が予め登録されている発信者情報と一致すること、アップロード指示メールが所定時間内に所定回数受信されること、等の少なくとも一つの条件を採用することができる。このような所定条件のチェックは、ヘッダ情報チェックのみでは認証が不十分である場合に採用することが好ましいが、必須ではない。

【００３５】

所定条件が満足されなければステップＳ６１１へ進み、通常のメール処理を行う。所定条件の満足が確認されたら、キー操作を無効化する（Ｓ６０５）。ついで、ネットワークにアクセスし、指定データをサーバへ送信する（Ｓ６０６）。送信が終了したら（Ｓ６０７，Ｙｅｓ）、指定データを消去する（Ｓ６０８）。ついで、指定データのアップロードおよび消去が完了したことを示す応答メールを前記アップロード指示メールの発信者に対して返信する（Ｓ６０９）。このよ

うな返信メールもテンプレートとして予め移動端末内に用意しておくことができる。その後、キー操作無効化を解除して（Ｓ６１０）、本処理を終了する。

【００３６】

このように、第２のデータアップロード処理では、移動端末外部からのアップロード指示メールにより、移動端末内の指定データのアップロードおよび消去が可能となる。

【００３７】

次に、図７により第３のデータアップロード処理について説明する。この第３のデータアップロード処理は第２のデータアップロード処理と同様、移動端末の正当なユーザが紛失等した当該移動端末を通信ネットワークを介して遠隔的に制御するものであるが、メールではなく音声通信によって行うものである。ここでは、通常、トーン信号と呼ばれるＤＴＭＦ(Dual Tone Multi-Frequency)信号を用いる。この信号は、電話機の各プッシュボタンに対応して得られるアナログ信号である。受信側では予め定められたのトーン信号列を受信したとき、外部からの所定の指示を認識することができる。

【００３８】

より具体的には、現在の携帯電話機のような移動端末には、何回か着信音が鳴る間に着信がない場合に、伝言メモ（留守番電話）モードへ遷移する機能が備わっており、この応答中に、トーン信号の入力を受け付け、指定されたトーン信号列を契機として、端末は本処理に移行することができる。または、伝言メモを受け付けた後に、自動応答モードに遷移し、入力を受け付ける。ここで、悪意の第三者が応答してしまう場合が考えられるが、その場合には自動応答モードに入ることができない。しかし、上記他のデータアップロード処理と併用すれば、この第３のデータアップロード処理も有用である。

【００３９】

図７において、移動端末が自動的に電話着信を行うと（Ｓ７０１，Ｙｅｓ）、自動応答モードに遷移し（Ｓ７０２）、認証処理を行う（Ｓ７０３）。これは例えばパスワード入力の受付、および照合チェックである。認証ＮＧであれば（Ｓ７０４，Ｎｏ）、回線を切断して（Ｓ７１３）、本処理を終了する。

【００４０】

認証ＯＫ（Ｓ７０４，Ｙｅｓ）であれば、コマンドを受け付ける（Ｓ７０５）。このコマンドが、データアップロードを指示する予め登録されたコマンドと一致しなければ（Ｓ７０６，Ｙｅｓ）、回線を切断して（Ｓ７１３）、本処理を終了する。回線切断の前に、数回のリトライを認めてもよい。ここでのコマンドは、好ましくは、端末のユーザが予め登録した数字列である。

【００４１】

コマンド一致が確認されたら（Ｓ７０６，Ｙｅｓ）、回線を切断し（Ｓ７０７）、データアップロードに移る。すなわち、キー操作を無効化し（Ｓ７０８）、指定データをサーバへ送信する（Ｓ７０９）。この送信が終了したら（Ｓ７１０，Ｙｅｓ）、端末内の指定データを消去する（Ｓ７１１）。その後、キー操作無効化を解除し（Ｓ７１２）、本処理を終了する。

【００４２】

自動応答モードに移行した後、回線接続中、通話相手の操作内容に対して、操作ガイドや操作結果を知らせるための予め用意された音声メッセージを発生するようにしてもよい。

【００４３】

ステップＳ７０７ではデータ通信のために一旦回線を切断したが、音声通話とデータ通信とが同時に行える場合には、ステップＳ７０７での回線切断を行わず、処理終了後に行うようにしてもよい。その場合には、アップロード処理完了の音声メッセージを送信することもできる。あるいは、予め当該正当ユーザのメールアドレス（端末に割り当てられたもの以外）を端末内に登録しておき、アップロード処理完了時にその旨の通知メールを当該メールアドレス宛に自動的に送信するようにしてもよい。

【００４４】

図８は、図７の第３のデータアップロード処理に対応する移動端末の構成例を示している。この構成は図２に示した構成に対して自動応答部１０９を追加したものである。自動応答部１０９は、少なくとも上述したようなトーン信号を受け付けてその識別を行う機能を備えるものであり、さらに好ましくは自動音声応答

の機能を備えるものである。他の構成は図２に示した構成と同じなので、説明は省略する。

【００４５】

図９は、上記のようにサーバに対してアップロードされたデータを、当該アップロードがなされた移動端末のユーザの指示により端末に復活させるデータダウンロード処理を示している。このデータダウンロード処理は、必ずしも当該データをアップロードした移動端末そのものである必要はなく、また、同機種の移動端末である必要もない。パーソナルコンピュータ（ＰＣ）のような他の端末からサーバにアクセスすることも可能である。

【００４６】

サーバ３００には認証時に用いるユーザ（ユーザＩＤ）毎のパスワードの設定がなされているものとする。移動端末１００は、基地局／制御局を介してサーバのホームページを閲覧できる。尚、指定ホームページのデータは、サーバ３００の外部記憶装置３０２に保存されている。指定ホームページに移動端末がアクセスすると（Ｓ９０１）、認証処理が行われる（Ｓ９０２）。認証処理では、例えば、移動端末の操作部１０６を用いてユーザ名とパスワードとが入力され、これらの入力情報は基地局／制御局を介して、サーバ３００に送信される。サーバにおける認証判定では、送信された情報と予めサーバに設定されているユーザ毎のパスワードとが比較される。入力されたユーザ名が存在しない場合、あるいは、存在してもそのパスワードが一致しない場合、認証誤りと判断され（Ｓ９０３，Ｎｏ）、その旨が端末へ通知される。この通知を受けて、端末はユーザに対してその旨を報知する（Ｓ９０４）。この報知の方法は、任意であり、例えば、端末の表示部へのメッセージ等の表示、ＬＥＤ等の光点灯、音の発生、振動の発生等のいずれかにより行える。

【００４７】

認証ＯＫであった場合（Ｓ９０３，Ｙｅｓ）、ユーザにダウンロード項目を選択させる（Ｓ９０５）。この際、各選択項目別に、保存先を選択できるようにしてもよい。選択された保存先にダウンロード項目と同じ名称のデータが存在する場合、同じデータが上書きされる。また、両データを比較し、データが全く同じ

場合は上書き保存を省略するようにしても良い。あるいは、上書き保存でなく、古い方のデータを新しい方のデータに一致させるよう、両データの同期をとるようにしてもよい。認証処理は、上記フロー中の位置ではなく、ステップＳ９０５の後に行うようにしてもよい。

【００４８】

ついで、この選択データがダウンロードされる（Ｓ９０６）。予め、アップロード対象のデータが固定的であり（例えば、アドレス帳、受信メールフォルダ１等）、選択の余地がない場合には、ステップＳ９０５，Ｓ９０６は不要である。

【００４９】

サーバから「終了の知らせ」を受信した際にダウンロードが終了する（Ｓ９０７，Ｙｅｓ）。このとき、ユーザに対して例えば表示部のメッセージ表示によりでダウンロード終了を報知し（Ｓ９０８）、本処理を終了する。ダウンロード終了したデータについては、サーバにおいてそのデータを消去するようにしてもよい。この消去は自動的に行ってもよいし、また、ユーザの指示または了解を得て行うようにしてもよい。

【００５０】

以上、本発明の好適な実施の形態について説明したが、上記で言及した以外にも、種々の変形、変更が可能である。

【００５１】

図５のステップＳ５０２の認証方法はパスワードによる認証を挙げたが、これに限るものではない。例えば、指紋認証用ＩＦを備える端末では、指紋認証を行うことができる。なお、正当なユーザに対して指紋認証が誤る可能性は低いので、一回の認証誤りで（リトライを認めず）不正アクセスと判断するようにしてもよい。

【００５２】

また、複数の認証方法を備える場合には、アクセス対象のデータに応じて、認証方法を変えるようにしてもよい。あるいは、複数の認証方法を組み合わせて用いるようにしてもよい。この場合、（ア）ひとつでも誤りとなったら、ステップＳ５０４へ移行する、（イ）認証誤り時に、よりセキュリティーレベルの高い認

証レベルの認証方法に変える、等の対処が考えられる。

【００５３】

データアップロード後に当該データの消去を行うようにしたが、データ消去は必ずしも行わなくてもよい。あるいは、予め、データの種類に応じて、消去を行うか否かを定めておいてもよい。この場合、消去を行うデータ種類を固定的に定めておく方法と、ユーザが選択的に定められるようにする方法とが考えられる。いずれにせよ、消去しない場合は、その後、少なくとも一定時間、当該データへのアクセスを不可とする（認証処理自体を抑止する）ことが好ましい。あるいは、これに代えて、複数の認証方法を用意しておき、セキュリティーレベルの低い認証方法から利用し、認証誤り後、よりセキュリティーレベルの高い認証方法を利用するようにしてもよい。データを消去しない場合、データのアップロードは不要であるが、端末紛失等の後も端末内データの利用を確保するためにアップロードを行ってもよい。

【００５４】

全てのデータにセキュリティーレベルを設定して、それを基に、指定データか否か、認証方法、認証誤り後の処理（消去の要否、アップロードの要否）を自動で設定するようにしてもよい。これをユーザがマニュアルで行うことも可能である。

【００５５】

上記説明では、アップロード対象をデータとしたが、アプリケーションレベルで指定できるようにしてもよい。この場合、アップロード対象は、そのアプリケーションの関連データとなる。

【００５６】

パスワードによる認証では、入力パスワードと登録パスワードの一致を条件としたが、質問形式による認証を行うことも可能である。すなわち、ユーザに対する質問に対してユーザがその質問に対して予め用意された回答と同じ回答をしたかどうかを条件とすることができる。

【００５７】

指定ホームページは、ユーザＩＤでアクセスするようにしたが、指定ホームペ

ージ（ＵＲＬ）をユーザ毎に設けることで、ユーザＩＤの入力を省略するようにすることも可能である。

【００５８】

図９のステップＳ９０４の後、当該指定ホームページからの該当ユーザ関連データのダウンロードを一定時間不可能にしてもよい。また、ユーザ名に該当するユーザに対してサーバが、ダウンロード要求時に認証誤りがあった旨のメールを送信するようにしてもよい。正当ユーザがパスワードを忘れて認証誤りとなった可能性があるので、そのメールでパスワードを再告知してもよい。

【００５９】

ステップＳ９０５で項目を選択後、選択されたデータを閲覧・編集できるようにしてもよい。他の機器からアクセスして、編集し、移動端末からダウンロードして同期を取れば、簡単にデータの更新を行う（例えばアドレス帳に新たな項目を入力する）ことができる。

【００６０】

【発明の効果】

本発明によれば、認証処理の否定的な結果を契機として即座に移動端末装置内のデータの待避および消去を行うことにより、移動端末のデータへの不正アクセス・使用を有効に防ぐことができる。

【００６１】

また、移動端末を紛失等した場合に、電子メールやトーン信号列による外部からの指示により、即座に移動端末のデータを待避および消去することができる。このために、位置登録局や基地局での特別な処理は必要ない。

【００６２】

これらの結果として、データのセキュリティに関して移動端末ユーザの安心感が増す。

【図面の簡単な説明】

【図１】

本発明が適用されるシステムのモデル例を示す図である。

【図２】

図１のシステム内の移動端末の構成例を示すブロック図である。

【図３】

図１のシステム内の基地局／制御局の構成例を示すブロック図である。

【図４】

図１のシステム内のサーバの構成例を示すブロック図である。

【図５】

本発明の実施の形態における第１のアップロード処理の処理例を示すフローチャートである。

【図６】

本発明の実施の形態における第２のアップロード処理の処理例を示すフローチャートである。

【図７】

本発明の実施の形態における第３のアップロード処理の処理例を示すフローチャートである。

【図８】

図７の第３のデータアップロード処理に対応する移動端末の構成例を示すブロック図である。

【図９】

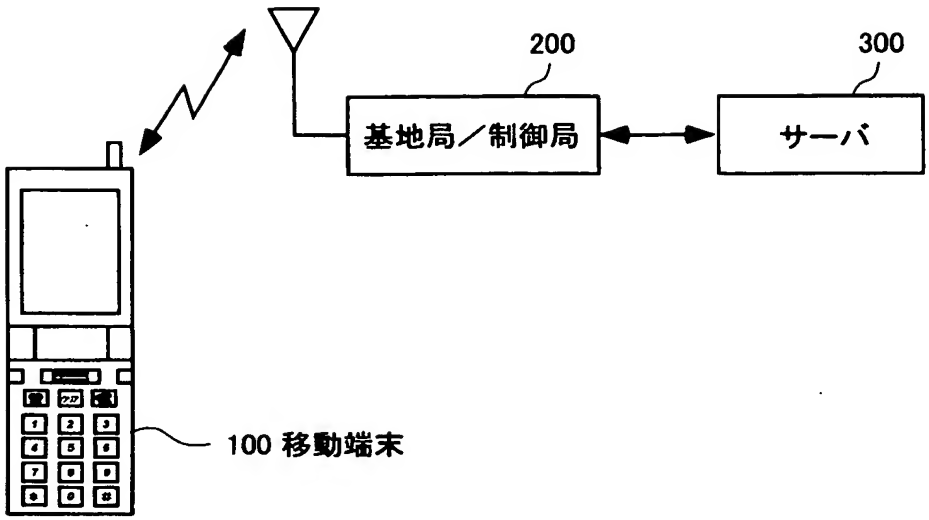
本発明の実施の形態におけるデータダウンロード処理を示すフローチャートである。

【符号の説明】

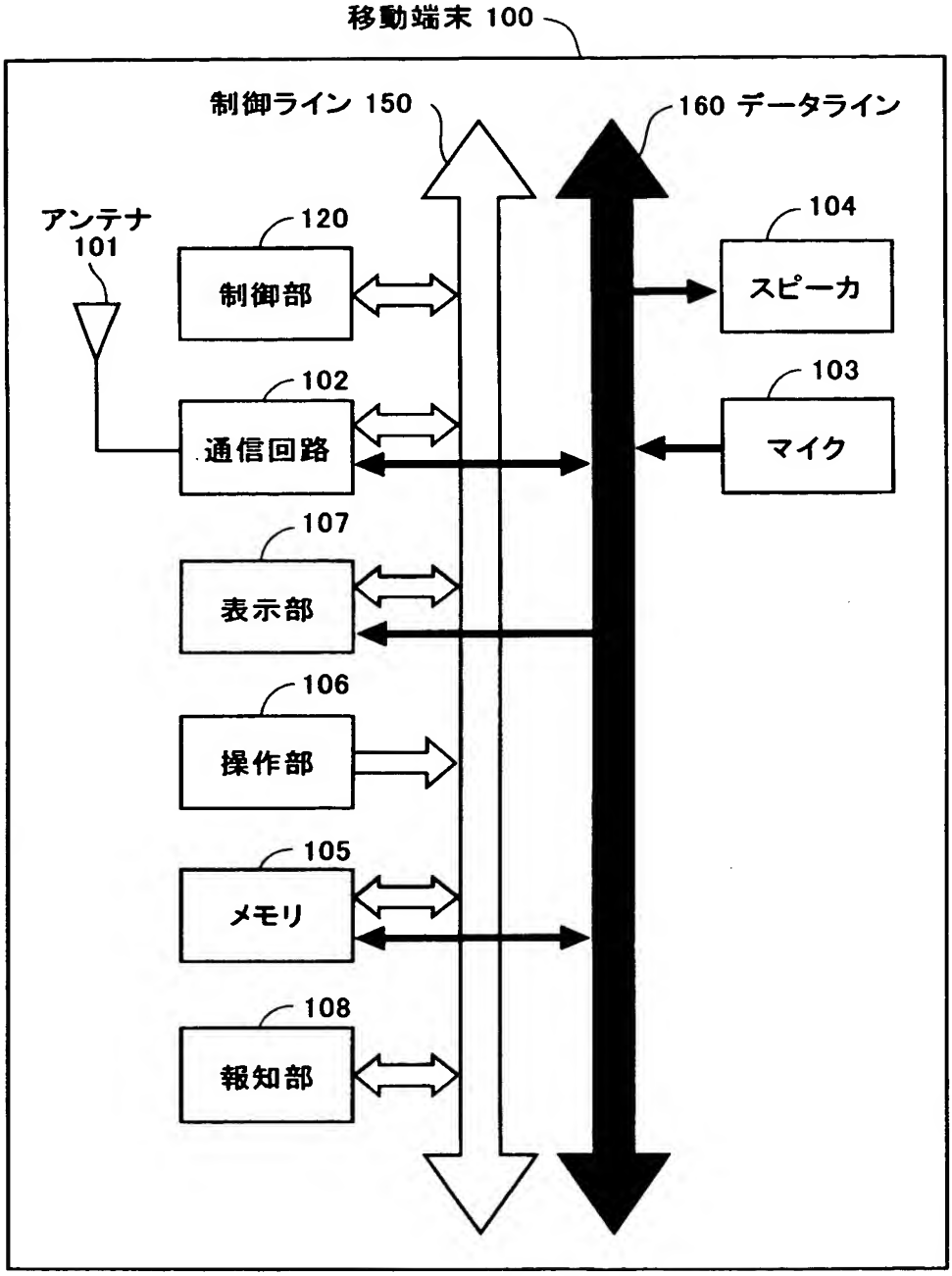
１００…移動端末装置、２００…基地局／制御局、３００…サーバ

【書類名】　図面

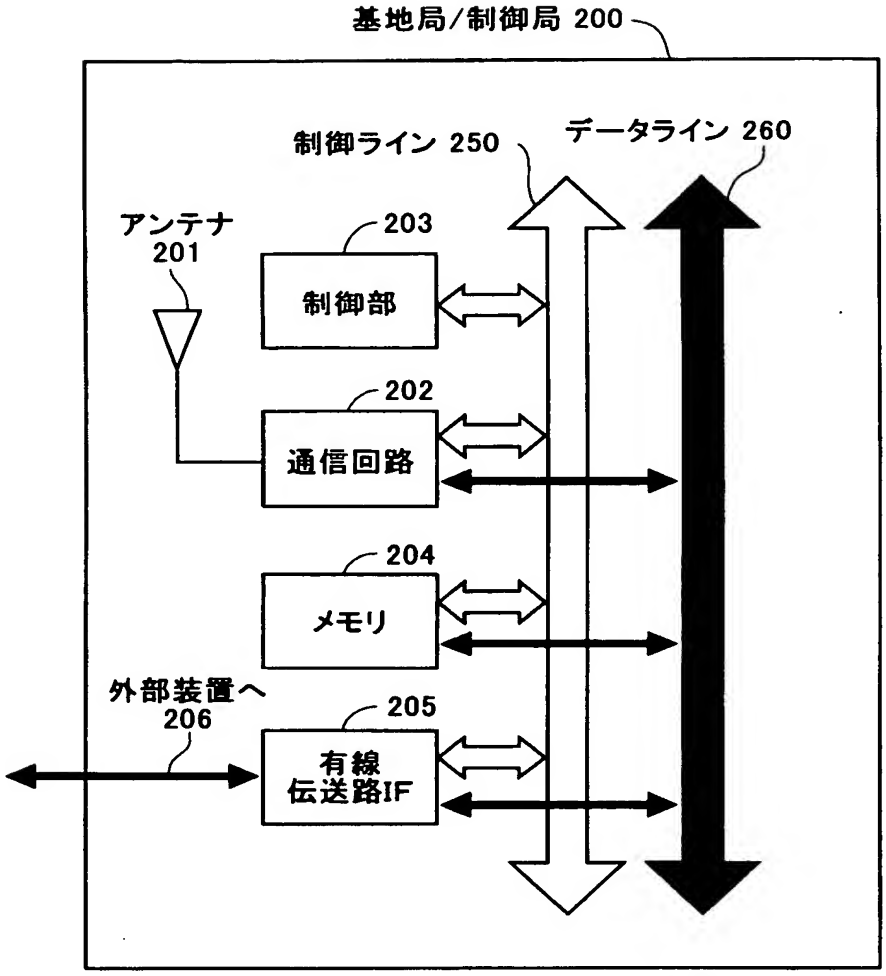
【図１】



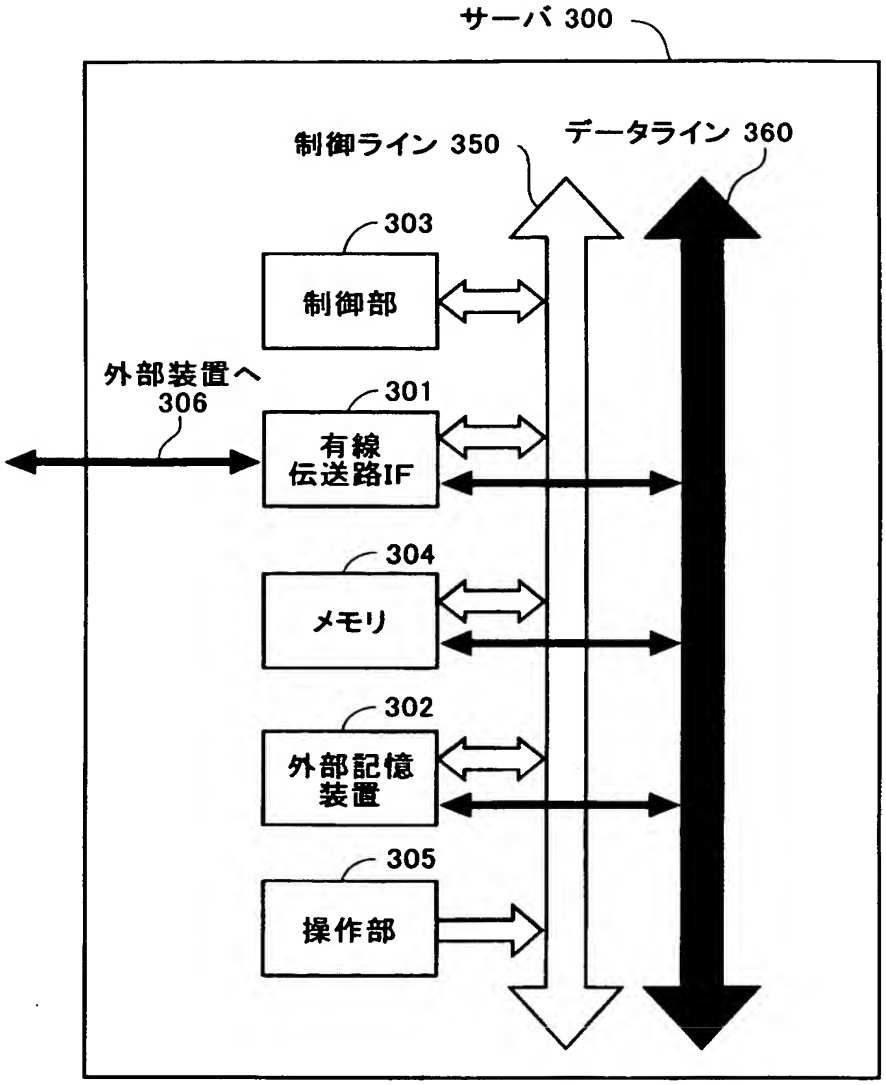
【図２】


移動端末 100
制御ライン 150
160 データライン
アンテナ
101
120
制御部
102
通信回路
107
表示部
106
操作部
105
メモリ
108
報知部
104
スピーカ
103
マイク

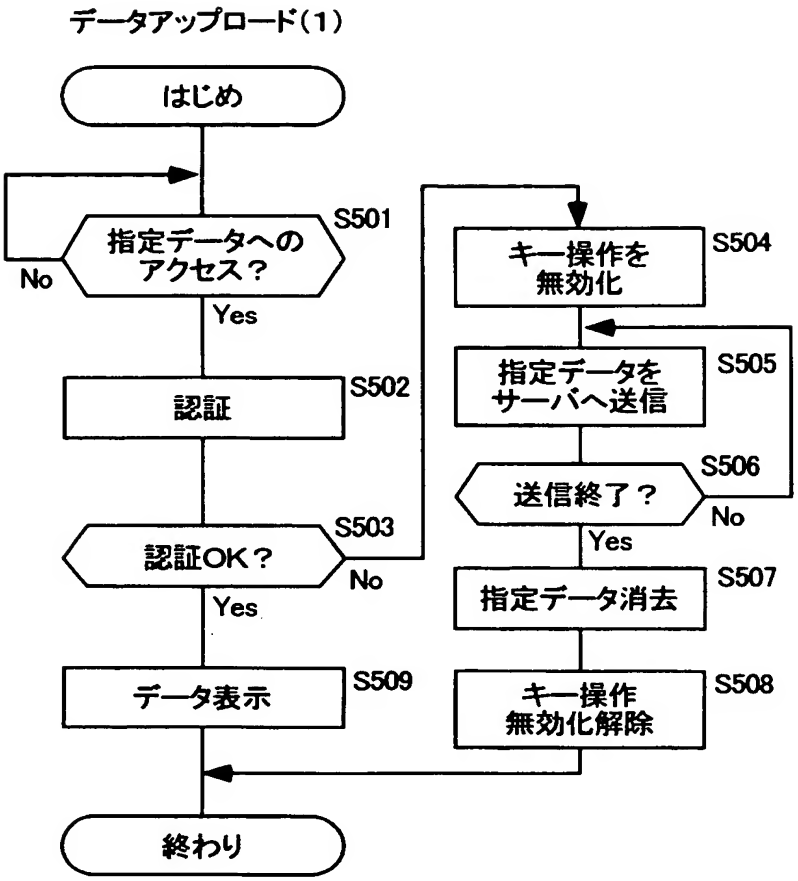
【図３】


基地局/制御局 200
制御ライン 250
データライン 260
アンテナ
201
203
制御部
202
通信回路
204
メモリ
外部装置へ
206
205
有線
伝送路IF

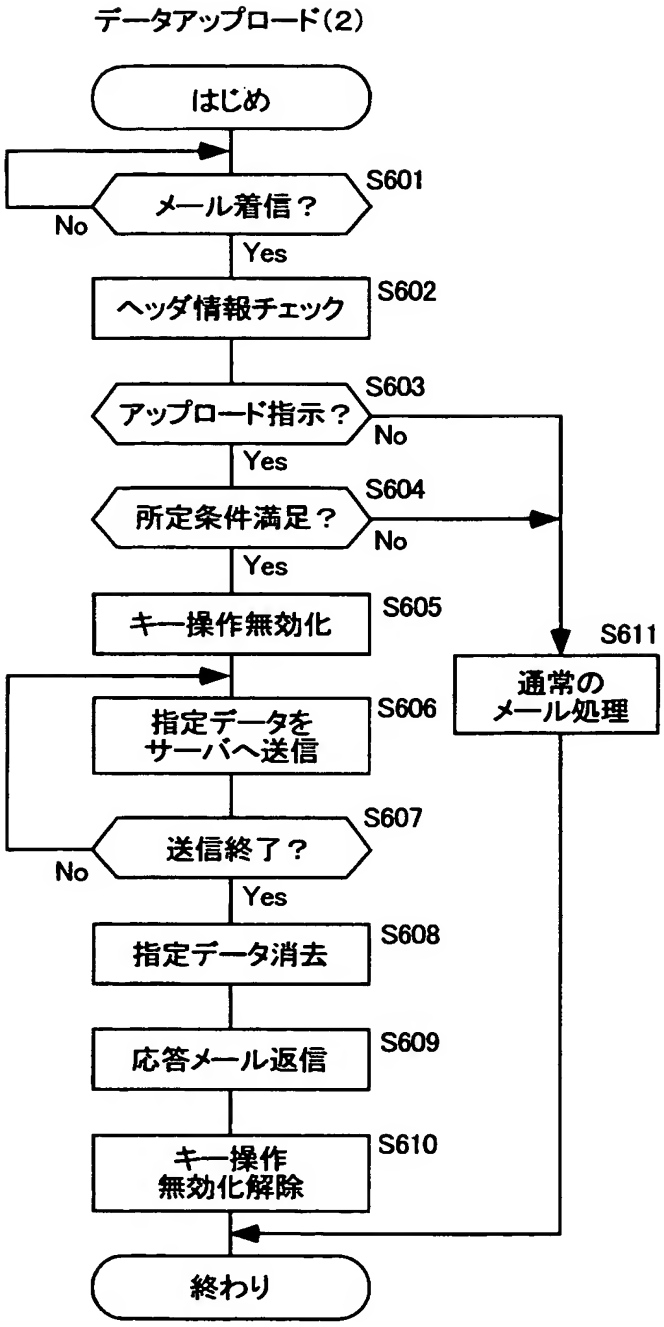
【図４】


サーバ 300
制御ライン 350
データライン 360
303
制御部
外部装置へ
306
301
有線
伝送路IF
304
メモリ
302
外部記憶
装置
305
操作部

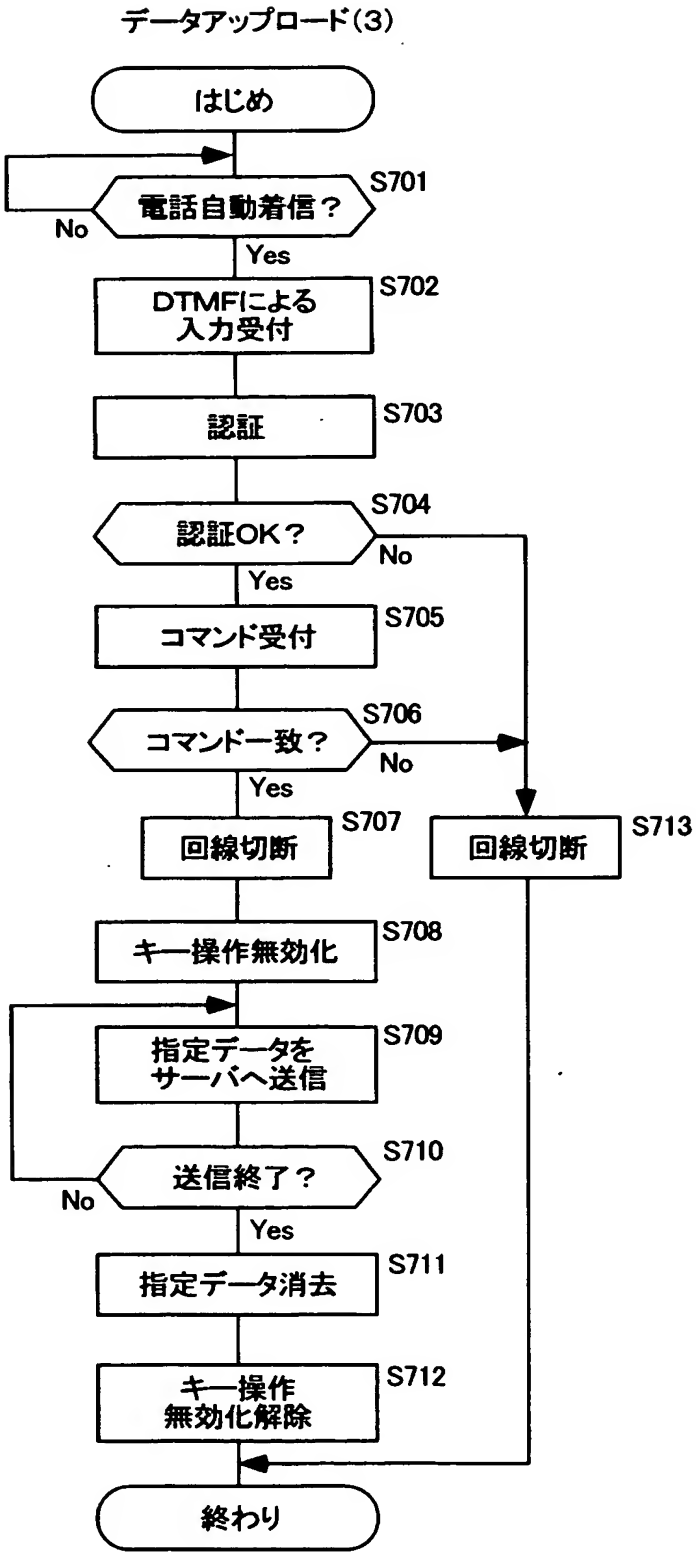
【図５】


データアップロード(1)
はじめ
S501
指定データへの
アクセス？
No
Yes
S502
認証
S503
認証OK？
No
Yes
S509
データ表示
終わり
S504
キー操作を
無効化
S505
指定データを
サーバへ送信
S506
送信終了？
No
Yes
S507
指定データ消去
S508
キー操作
無効化解除

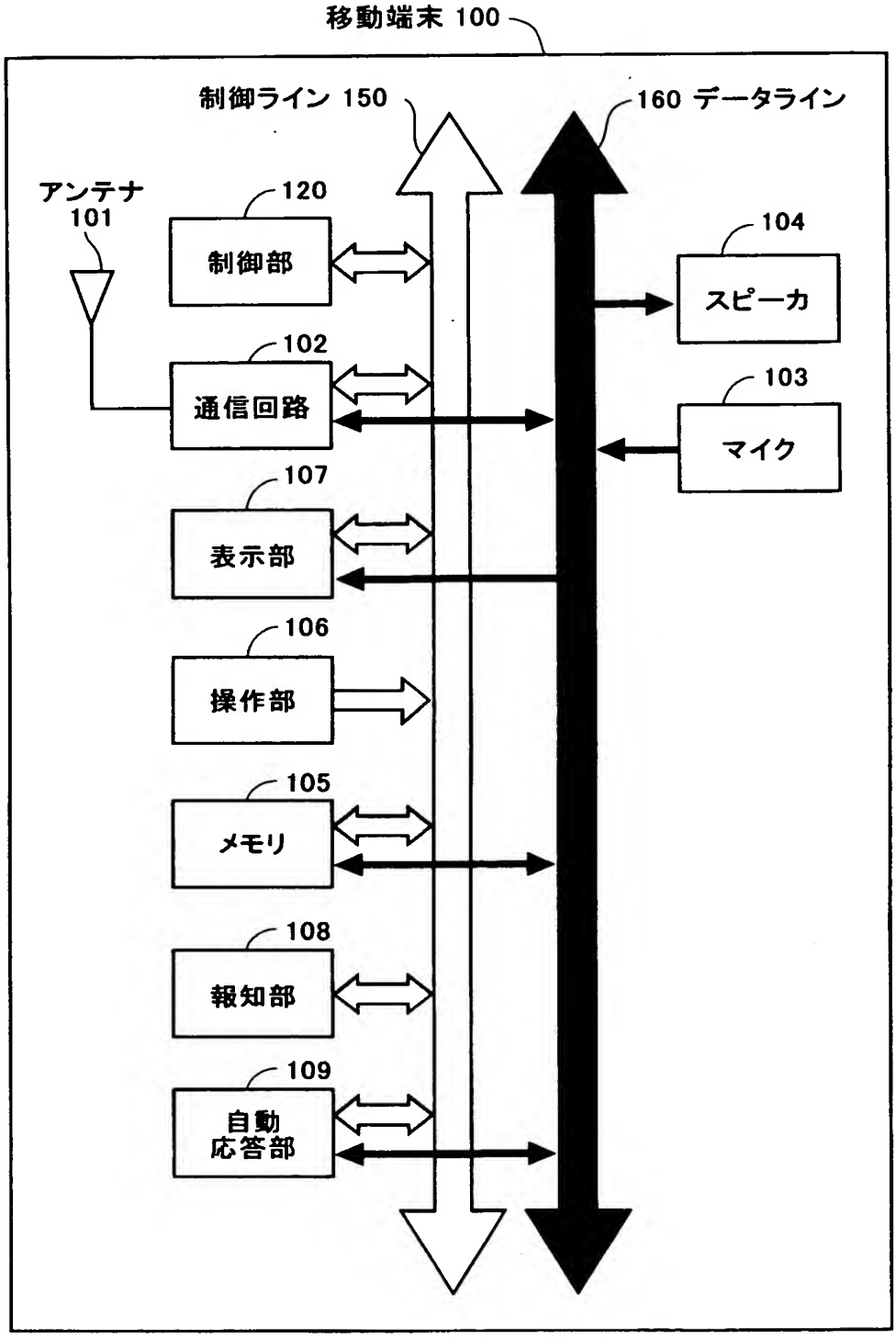
【図６】


データアップロード(2)
はじめ
S601
メール着信？
No
Yes
S602
ヘッダ情報チェック
S603
アップロード指示？
No
Yes
S604
所定条件満足？
No
Yes
S605
キー操作無効化
S606
指定データを
サーバへ送信
S607
送信終了？
No
Yes
S608
指定データ消去
S609
応答メール返信
S610
キー操作
無効化解除
S611
通常の
メール処理
終わり

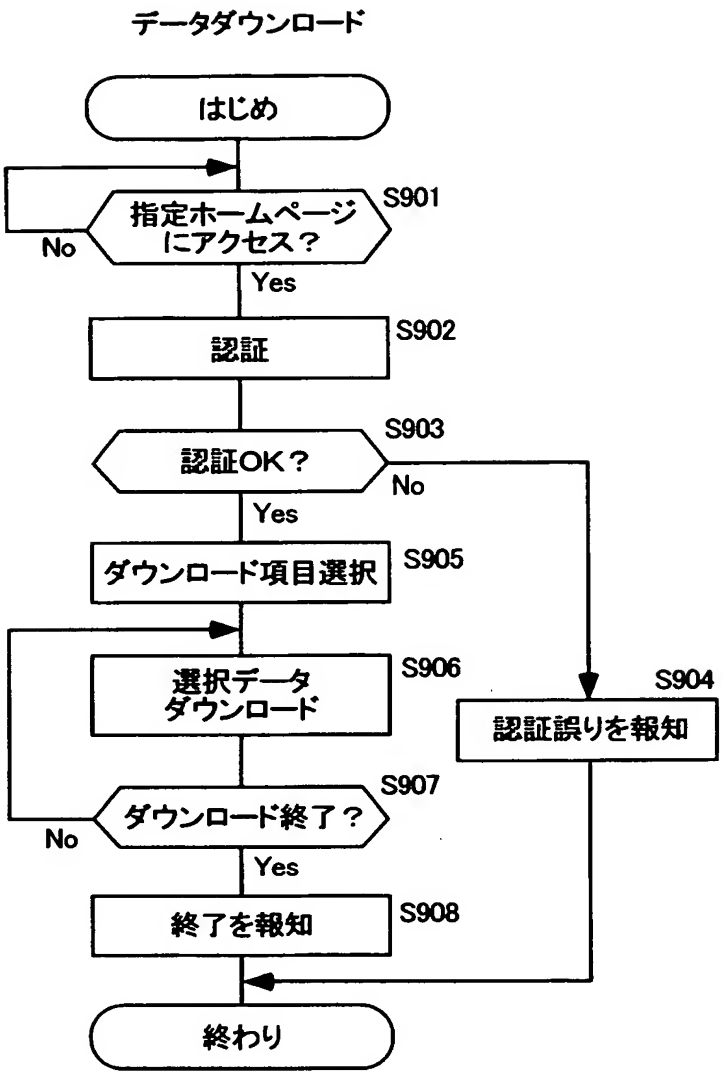
【図７】


データアップロード(3)
はじめ
電話自動着信？
S701
No
Yes
DTMFによる
入力受付
S702
認証
S703
認証OK？
S704
No
Yes
コマンド受付
S705
コマンド一致？
S706
No
Yes
回線切断
S707
回線切断
S713
キー操作無効化
S708
指定データを
サーバへ送信
S709
送信終了？
S710
No
Yes
指定データ消去
S711
キー操作
無効化解除
S712
終わり

【図８】


移動端末 100
制御ライン 150
160 データライン
アンテナ
101
120
制御部
102
通信回路
107
表示部
106
操作部
105
メモリ
108
報知部
109
自動
応答部
104
スピーカ
103
マイク

【図９】


データダウンロード
はじめ
S901
指定ホームページにアクセス？
No
Yes
S902
認証
S903
認証OK？
No
Yes
S905
ダウンロード項目選択
S906
選択データダウンロード
S904
認証誤りを報知
S907
ダウンロード終了？
No
Yes
S908
終了を報知
終わり

【書類名】　　要約書

【要約】

【課題】内部のデータを不正に閲覧しようとする者からデータを保護する。

【解決手段】移動端末装置１００は、ユーザの操作に基づいてそのユーザが正当なユーザであるか否かをチェックし、その認証の結果が否定的であるとき、メモリに記憶されたデータのうち、予め定められたデータを、予め定められたサーバ３００に対してアップロードし、この送信完了後に当該データをメモリから消去する。外部から移動端末装置１００に対する電子メールまたは電話によるトーン信号列によりデータのアップロードおよび消去を指示することも可能である。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２００３－０６１２３３
受付番号	５０３００３７３３５８
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１５年　３月１０日

＜認定情報・付加情報＞

【提出日】　平成15年 3月 7日

次頁無

特願２００３－０６１２３３

出　願　人　履　歴　情　報

識別番号　　［５０１４３１０７３］

１．変更年月日　　２００１年１１月　６日
［変更理由］　　新規登録
住　所　　東京都港区港南１丁目８番１５号　Ｗビル
氏　名　　ソニー・エリクソン・モバイルコミュニケーションズ株式会社